06-14-00

A

ATTORNEY DOCKET NO. 14102.0002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

NEEDLE & ROSENBERG, P.C.
Suite 1200, The Candler Building
127 Peachtree Street, N.E.
Atlanta, Georgia 30303-1811

June 13, 2000

Dear Sir:

Transmitted herewith for filing are the specification and claims of the utility patent application of:

Inventor(s): Nicolas J. Hammond

Title of Invention: METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY

Also enclosed are:

2	SHEETS OF	[X] FORMAL DRAWINGS	[] INFORMAL DRAWINGS
X	OATH OR DECLARATION OF APPLICANT(S)		
X	A POWER OF ATTORNEY		
	A PRELIMINARY AMENDMENT		
	A VERIFIED STATEMENT TO ESTABLISH SMALL ENTITY STATUS UNDER 37 C.F.R. §1.9 AND §1.27		
X	A CHECK IN THE AMOUNT OF $690.00 TO COVER THE FILING FEE.		
X	THE COMMISSIONER IS HEREBY AUTHORIZED TO CHARGE ANY ADDITIONAL FEES WHICH MAY BE REQUIRED IN CONNECTION WITH THE FOLLOWING OR CREDIT ANY OVERPAYMENT TO ACCOUNT NO. 14-0629		
	A CERTIFIED COPY OF PREVIOUSLY FILED FOREIGN APPLICATION NO. FILED IN ON .		
X	I hereby certify that this correspondence is being placed in the United States Mail as Express Mail No. EL403199825US on 13 day of JUNE, 2000. Everardo McFarlane — 6-13-2000 DATE		
	A computer readable form of the sequence listing in compliance with 37 C.F.R. § 1.821(e). The content of the computer readable form of the sequence listing and the sequence listing in the specification of the application as filed are the same.		
	OTHER (IDENTIFY)		

The filing fee is calculated as follows:

CLAIMS AS FILED, LESS ANY CLAIMS CANCELLED BY AMENDMENT

TOTAL CLAIMS = 10 - 20 = 0 x $18.00 =	$0
INDEPENDENT CLAIMS = 3 - 3 = 0 x $78.00 =	$0
BASIC FEE =	$690.00
TOTAL OF ABOVE CALCULATIONS =	$690.00
REDUCTION BY 1/2 FOR SMALL ENTITY =	$0
TOTAL FILING FEE =	$690.00

Respectfully submitted,

Sumner C. Rosenberg
Registration No. 28,753

NEEDLE & ROSENBERG, P.C.
Suite 1200, The Candler Building
127 Peachtree Street, N.E.
Atlanta, Georgia 30303-1811
(404) 688-0770

Express Mail No. EL403199825US
Attorney Docket No. 14102.0002
NON-PROVISIONAL PATENT

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TO ALL WHOM IT MAY CONCERN:

Be it known that I, **Nicolas J. Hammond,** having a post office address and a residence address at 211 East Wesley Road, Atlanta, Georgia 30305-3774, a citizen of the United Kingdom, have invented new and useful improvements in a

METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY

for which the following is a specification.

ATTORNEY DOCKET NO. 14102.0002

METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to copending provisional application Serial No. 60/146,175, filed July 29, 1999, which is incorporated by reference, and claims the benefit of its earlier filing date under 35 USC Section 119(e).

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer network security and, more specifically, to a method and apparatus for auditing computer network security.

2. Description of the Prior Art

As use of large computer networks becomes more prevalent, computer security increases in importance. To reduce networked computer vulnerability, many organizations run periodic security audit scans of their computer systems. Such scans typically involve a dedicated scanning machine that attempts to gain unauthorized access to a computer system via a computer network through a variety of methods. The scanning machine will make numerous attempts to gain access and maintain a record of any security breaches that it detects.

Conventional scanning systems perform scans on command and are frequently dedicated to only a single user. Thus, scans are not performed periodically unless the user remembers to activate the scanning machines. Furthermore, many scanning machines are idle for large periods of time.

Therefore, there is a need for a scanning system that periodically schedules security scans of several users.

SUMMARY OF THE INVENTION

The disadvantages of the prior art are overcome by the present invention which, in one aspect, is an apparatus for auditing security of a computer system. At least one secure application server is in communication with a global computer network. The secure application server is programmed to receive selectively security audit instruction data from the remote computer system via the global computer network. A plurality of scanning machines each are in communication with the global computer network and are programmed to execute selectively a security audit scan of the remote computer system via the global computer network. A central computer, having a memory, is configured as a database server and as a scheduler. The central computer is in communication with the secure application server and the scanning machine. The central computer is programmed to perform the following operations: evaluate a database to determine if a security audit scan is currently scheduled to be run for a user; determine which of the plurality of scanning machines is available to perform a security audit scan; copy scan-related information into a scanning machine determined to be available and instruct the scanning machine to begin scan; and record the results of the scan in the memory.

In another aspect, the invention is a method of auditing security of a computer system in which an instruction to perform a security audit scan on a computer system is received from a user via a global computer network. A scanning machine is instructed to access the remote computer system via the global computer network and thereby perform a security audit scan of the remote computer system. At least one result of the security audit scan is reported to the user once the security audit scan is complete.

In yet another aspect, the invention is a method of auditing computer system security in which a database is accessed to determine when a security audit scan of a computer system is to be executed. Upon determining that a security audit scan of the remote computer system is to be executed, security audit scan data is copied into a scanning system, the scanning system is caused to establish communication with the remote computer system via a global computer network and to execute a security audit scan of the remote computer system via the global computer network. A result of the security audit scan of the global computer network is stored and a message is transmitted to a user of the remote computer system that indicates the result of the security audit scan.

These and other aspects of the invention will become apparent from the following description of the preferred embodiments taken in conjunction with the following drawings. As would be obvious to one skilled in the art, many variations and modifications of the invention may be effected without departing from the spirit and scope of the novel concepts of the disclosure.

BRIEF DESCRIPTION OF THE FIGURES OF THE DRAWINGS

FIG. 1 is a schematic diagram of the devices employed in one embodiment of the invention.

FIG. 2 is a flow chart showing the steps executed in one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the invention is now described in detail. Referring to the drawings, like numbers indicate like parts throughout the views. As

used in the description herein and throughout the claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise: the meaning of "a," "an," and "the" includes plural reference, the meaning of "in" includes "in" and "on." Also, as used herein, "global computer network" includes the Internet. A "secure application server" could include any digital machine that controls a computer communication and includes security features that inhibit unauthorized access.

As shown in FIG. 1, one embodiment of an apparatus **100** for auditing security of a remote computer system **102** or a remote network **104** is resident at a central site **110**. A central computer **120**, including a computer-readable memory, is configured as a database server and acts as a scheduler. The central computer **120** is in communication with at least one secure application server **130** and a plurality of scanning machines **140**, of the type generally known in the art of computer network security analysis. The secure application server **130** (for example, an Internet Web server) is in communication with a global computer network **106** (such as the Internet) and is programmed to receive selectively security audit instruction data from the remote computer system **102** via the global computer network **106**. A plurality of scanning machines **140a-n** is in communication with the global computer network **106** and each is programmed to execute selectively a security audit scan of the remote computer system **102** via the global computer network **106**. A security audit scan could include, but is not limited to, any combination of the following forms of security assessments generally known to the art of computer network security analysis: security audit scan; security scan; audit; audit scan; remote assessment; vulnerability assessment; vulnerability analysis; and penetration study.

As shown in FIG. 2, one illustrative embodiment of the general procedure executed by the central computer **120** includes assigning **200** the value of zero to an iteration variable and performing a test **202** to determine whether a security audit scan is scheduled for the current period. If a scan is not scheduled, the central

computer **120** performs a test **118** to determine if a user has requested a scan. If a scan is scheduled, or if the user has requested a scan, the central computer finds the next available scanning machine by iteratively performing a test **204** to determine if the scanning machine designated as the current value of the iteration variable is available and, if it is not available, incrementing **206** the iteration variable and returning the thread of execution to test **204**. When a scanning machine is found to be available, the necessary scan related information is copied **208** from the central computer **120** to the scanning machine and a message is e-mailed **210** to the user that indicates that a scan is scheduled and that the scan is commencing. The central computer **120** then instructs **220** the scanning system to establish communication with the remote computer system via a global computer network and commence the scan.

Once the scanning machine begins performing the scan, the central computer **120** repeatedly performs a test **212** to determine whether a "scan complete" indication is received from the scanning machine. If a "scan complete" indication is received, then an e-mail is sent to the user **214** indicating that the scan is complete. The results of the scan are then recorded **216** in a database resident in the central computer **120** or on a file system of another database machine. The results could include an indication that the scan is complete, the date and time of the scan, the nature of the tests performed during the scan and the nature of any deficiencies detected by the scan. The results of the scan may then be used for generating a scan report and other uses, such as statistical analyses, *etc.*

While one illustrative embodiment of the procedure executed by the central computer **120** is shown in FIG. 2, it will be readily understood that many other scan scheduling algorithms could be employed without departing from the scope of the invention so long as the algorithm employed provides for scheduling a scan of a remote system, selecting an available scanning machine and instructing the selected scanning machine to execute a scan via a global computer network.

The above described embodiments are given as illustrative examples only. It will be readily appreciated that many deviations may be made from the specific embodiments disclosed in this specification without departing from the invention. Accordingly, the scope of the invention is to be determined by the claims below rather than being limited to the specifically described embodiments above.

CLAIMS

What is claimed is:

1. An apparatus for auditing security of a remote computer system, comprising:
   a. at least one secure application server in communication with a global computer network and programmed to receive selectively security audit instruction data from the remote computer system via the global computer network;
   b. a plurality of scanning machines in communication with the global computer network and programmed to execute selectively a security audit scan of the remote computer system via the global computer network; and
   c. a central computer, having a memory, configured as a database server and as a scheduler, in communication with the secure application server and the scanning machine, programmed to perform the following operations:
      a. evaluate a database to determine if a security audit scan is currently scheduled to be run for a user;
      b. determine which of the plurality of scanning machines is available to perform a security audit scan;
      c. copy scan-related information into a scanning machine determined to be available and instruct the scanning machine to begin scan; and
      d. record the results of the scan in the memory.

2. The apparatus of Claim 1, wherein the secure application server comprises a Web server.

3. The apparatus of Claim 1, wherein the central computer is further programmed to notify the user via e-mail that a scan is commencing.

4. The apparatus of Claim 1, wherein the central computer is further programmed to update database to indicate that scan is complete

5. The apparatus of Claim 1, wherein the central computer is further programmed to notify the user of a completion of a scan.

6. The apparatus of Claim 1, wherein when the central computer performs the operation in which the central computer records the results of the scan, the central computer also copies the data to the database and copies the report to the file system on the database machine when scan is complete.

7. A method of auditing security of a computer system, comprising the steps of:
   a. receiving from a user, via a global computer network, an instruction to perform a security audit scan on a computer system;
   b. instructing a scanning machine to access the remote computer system via the global computer network and thereby perform a security audit scan of the remote computer system; and
   c. reporting at least one result of the security audit scan to the user once the security audit scan is complete.

8. The method of Claim 7, further comprising the step of recording the result of the security audit in a computer memory.

9. The method of Claim 7, further comprising the step of evaluating which of a plurality of scanning machines is available to perform the security audit scan.

10. A method of auditing computer system security, comprising the steps of:
   a. accessing a database to determine when a security audit scan of a computer system is to be executed;
   b. upon determining that a security audit scan of the remote computer system is to be executed, performing the following steps:

i. copying security audit scan data into a scanning system;

ii. causing the scanning system to establish communication with the remote computer system via a global computer network;

iii. causing the scanning system to execute a security audit scan of the remote computer system via the global computer network; and

iv. storing a result of the security audit scan of the global computer network; and

b. transmitting a message to a user of the remote computer system that indicates the result of the security audit scan.

ABSTRACT

In an apparatus for auditing security of a computer system, at least one secure application server is in communication with a global computer network. The secure application server is programmed to receive selectively security audit instruction data from a remote computer system via the global computer network. A plurality of scanning machines each are in communication with the global computer network and are programmed to execute selectively a security audit scan of the remote computer system via the global computer network. A central computer, having a memory, is configured as a database server and as a scheduler. The central computer is in communication with the secure application server and the scanning machine. The central computer is programmed to perform the following operations: evaluate a database to determine if a security audit scan is currently scheduled to be run for a user; determine which of the plurality of scanning machines is available to perform a security audit scan; copy scan-related information into a scanning machine determined to be available and instruct the scanning machine to begin scan; and record the results of the scan in the memory.

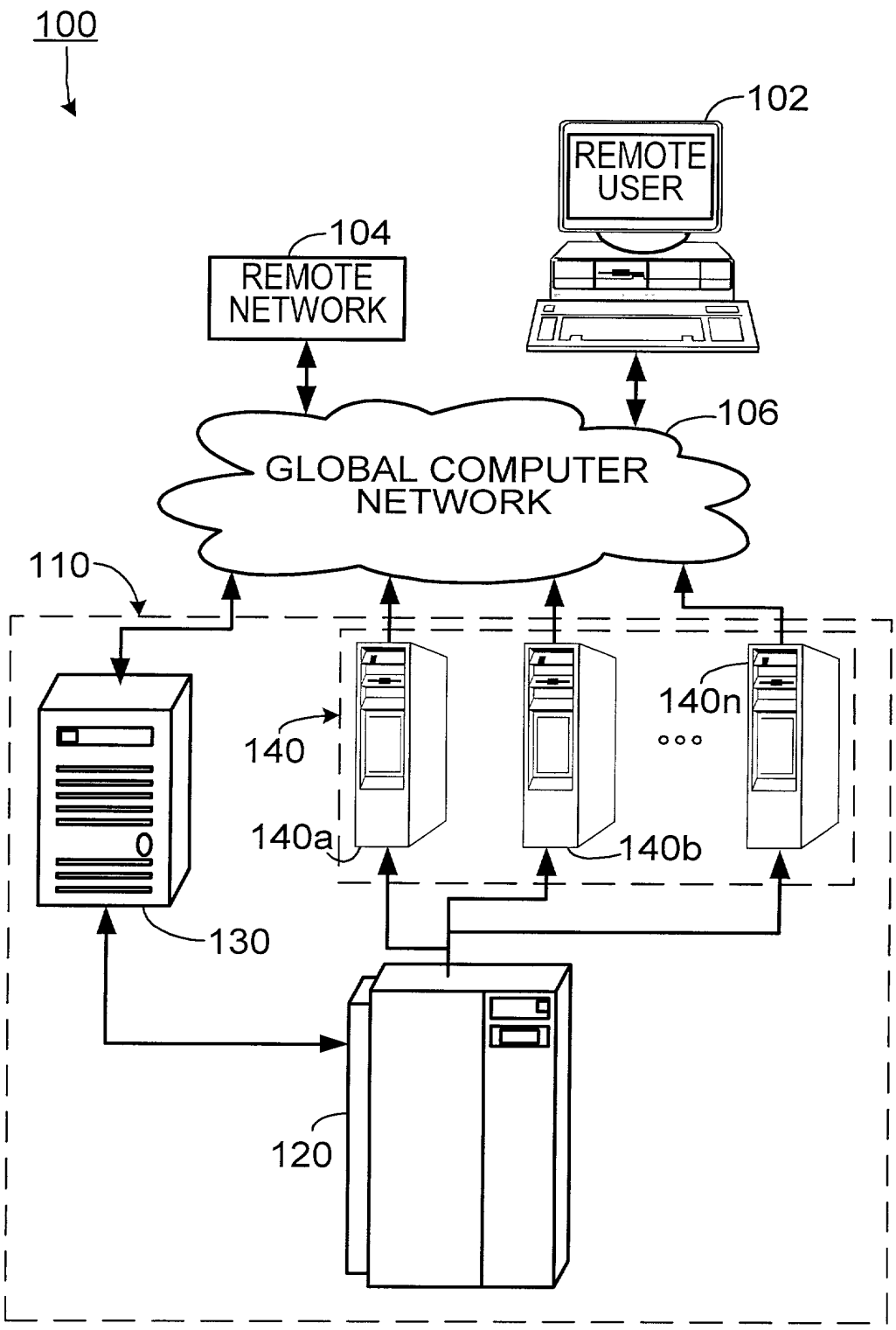
100
102
REMOTE USER
104
REMOTE NETWORK
106
GLOBAL COMPUTER NETWORK
110
140
140a
140b
140n
130
120

FIG. 1

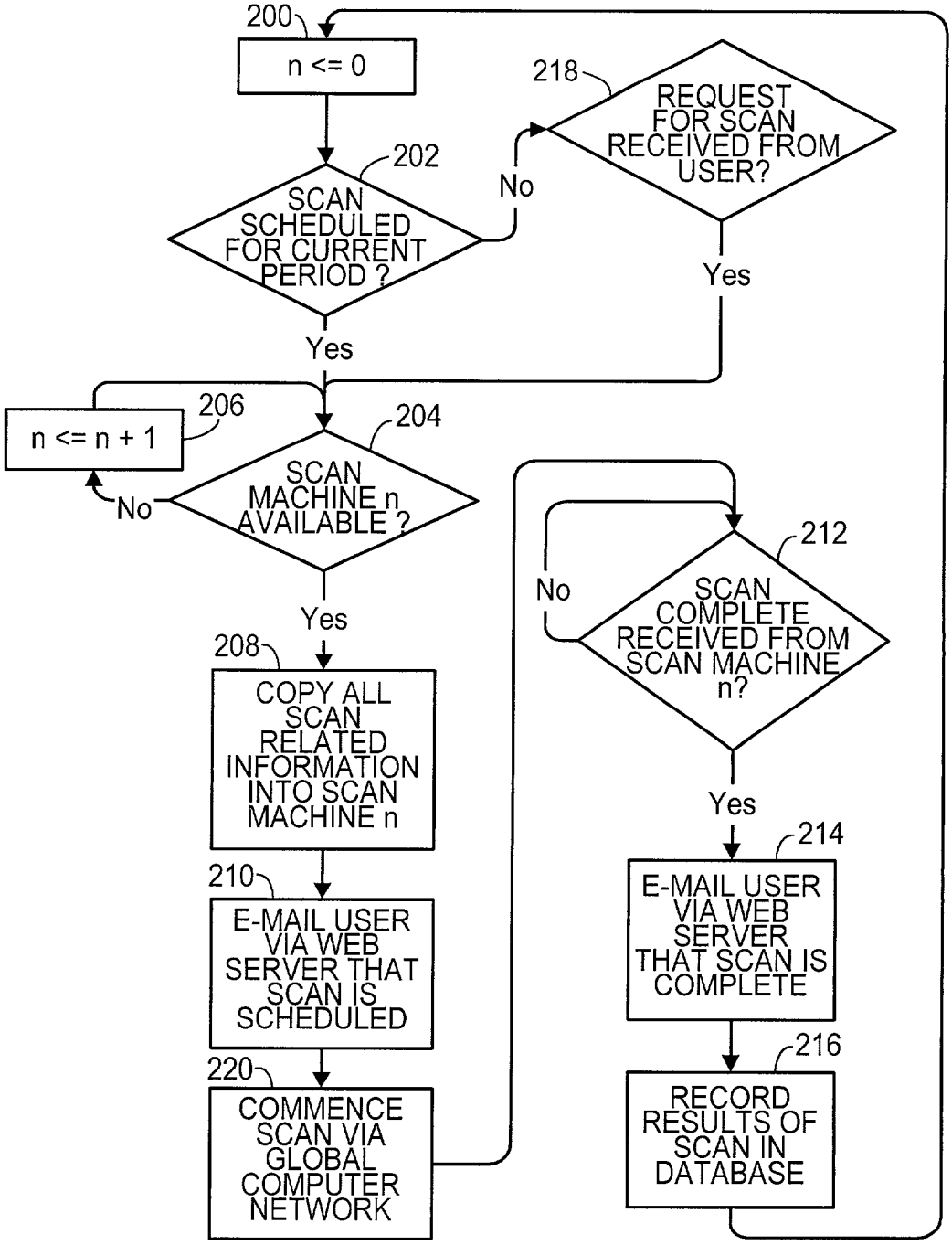
200
n <= 0
202
SCAN SCHEDULED FOR CURRENT PERIOD ?
No
218
REQUEST FOR SCAN RECEIVED FROM USER?
Yes
Yes
206
n <= n + 1
204
SCAN MACHINE n AVAILABLE ?
No
Yes
208
COPY ALL SCAN RELATED INFORMATION INTO SCAN MACHINE n
210
E-MAIL USER VIA WEB SERVER THAT SCAN IS SCHEDULED
220
COMMENCE SCAN VIA GLOBAL COMPUTER NETWORK
212
SCAN COMPLETE RECEIVED FROM SCAN MACHINE n?
No
Yes
214
E-MAIL USER VIA WEB SERVER THAT SCAN IS COMPLETE
216
RECORD RESULTS OF SCAN IN DATABASE

FIG. 2

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

(X) Original () Supplemental () Substitute () PCT

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **"METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY"** which is described and claimed in the specification

(check one) [X] which is attached hereto, or
[] which was filed on as United States Application No. , or
[ ] in International Application No. PCT/, filed, and as amended on (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information known by me to be material to the patentability of the claims of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a) - (d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate relating to this subject matter having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATIONS: (ENTER BELOW IF APPLICABLE)			PRIORITY CLAIMED (MARK APPROPRIATE BOX BELOW)	
APP. NUMBER	COUNTRY	DAY/MONTH/YEAR FILED	YES	NO
N/A				

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

APPLICATION NUMBER	FILING DATE
60/146,175	7/29/99

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information known by me to be material to the patentability of the claims of this application as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS (MARK APPROPRIATE COLUMN BELOW)		
		PATENTED	PENDING	ABANDONED
N/A				

I hereby appoint the following attorneys and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

William H. Needle	Reg. No. 26,209	Charles H. Fails	Reg. No. 37,616
Sumner C. Rosenberg	Reg. No. 28,753	Jacqueline M. Hutter	Reg. No. 44,792
David G. Perryman	Reg. No. 33,428	David S. Kerven	Reg. No. 43,712
Mitchell A. Katz	Reg. No. 33,919	Lori L. Kerber	Reg. No. 41,113
Gregory J. Kirsch	Reg. No. 35,572	Janice A. Kimpel	Reg. No. 42,734
Gwendolyn D. Spratt	Reg. No. 36,016	Lawrence D. Maxwell	Reg. No. 35,276
Nagendra Setty	Reg. No. 38,300	Tina W. McKeon	Reg. No. 43,791
D. Andrew Floam	Reg. No. 34,597	Mary L. Miller	Reg. No. 39,303
William R. Johnson	Reg. No. 32,875	Mark A. Murphy	Reg. No. 42,915
Allan G. Altera	Reg. No. 40,274	Lance D. Reich	Reg. No. 42,097
Shari Corin	Reg. No. 46,243	Lisa A. Samuels	Reg. No. 43,080
Kean J. DeCarlo	Reg. No. 39,954	Lawrence A. Villanueva	Reg. No. 43,968
LaVonda R. DeWitt	Reg. No. 40,396	Mitchell G. Weatherly	Reg. No. 40,864
		Tim T. Xia	Reg. No. 45,242

Address all telephone calls to Sumner C. Rosenberg, Esq. at telephone no. (404) 688-0770.

Address all correspondence to:

Sumner C. Rosenberg, Esq.
NEEDLE & ROSENBERG, P.C.
Suite 1200, The Candler Building
127 Peachtree Street, N.E.
Atlanta, Georgia 30303-1811

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: **Nicolas J. Hammond**

Inventor's signature: _____ Date: April 4th, 2000

Residence: 211 East Wesley Road, Atlanta, Georgia 30305-3774

Post Office Address: 211 East Wesley Road, Atlanta, Georgia 30305-3774

Citizenship: United Kingdom